MANTECH Publications

Journal of Blockchain Systems and Smart Contracts
Volume 2, Issue 2, May-August 2026
ISSN: 3139-132X (Online)

Smart Contract-Driven Decentralized Autonomous Organizations (DAOs): Governance Models, Security Challenges, and Future Applications

Hrishikesh Bapat[1], Harini Subramaniam[2]

ABSTRACT

Decentralized Autonomous Organizations (DAOs) represent a paradigm shift in organizational governance, leveraging immutable smart contracts on public blockchains to execute rules, allocate capital, and manage collective decision-making without centralized intermediaries. Despite rapid deployment across Decentralized Finance (DeFi), Venture Capital, and digital public goods, DAOs encounter severe structural, economic, and security vulnerabilities. This comprehensive review paper provides an analytical evaluation of smart contract-driven DAOs. We categorize and systematically compare primary governance models—including 1-Token-1-Vote, Quadratic Voting, Futarchy, and Delegation Mechanisms—highlighting their trade-offs regarding decentralization, Sybil resistance, capital efficiency, and voting turnout. Furthermore, we dissect key smart contract attack vectors such as governance flash loan manipulation, reentrancy vulnerabilities, proposal hijacking, and administrative access control breaches. Utilizing empirical case studies of major exploits (including The DAO, Beanstalk Farms, and Compound Governance), we evaluate defense architectures, including formal verification, multi-signature timelocks, and programmatic circuit breakers. Finally, the paper explores emerging application domains in decentralized science (DeSci) and supply chain management, outlining strategic pathways toward adaptive governance systems.

KEYWORDS: *Decentralized Autonomous Organizations (DAOs), Smart Contracts, Blockchain Governance, Quadratic Voting, Security Vulnerabilities, Flash Loan Attacks, Formal Verification.*

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

INTRODUCTION

The emergence of blockchain technology and Turing-complete smart contract platforms like Ethereum has enabled novel paradigms for decentralized coordination [1]. Decentralized Autonomous Organizations (DAOs) are internet-native, member-owned entities governed by immutable smart contracts rather than traditional hierarchical administrative structures [2]. By encoding governance rules, membership rights, and treasury dispatch mechanisms directly into self-executing code, DAOs establish trust-minimized, transparent, and censorship-resistant operational environments [3].

Over the past decade, DAOs have scaled dramatically, managing billions of dollars in treasury assets across Decentralized Finance (DeFi) protocols, asset management, and digital collectives [4]. However, the programmatic nature of DAOs presents a dual-edged sword: while automated execution removes reliance on human escrow agents, it introduces critical software vulnerabilities. The principle of 'code is law' implies that software bugs, flawed economic incentives, or malicious proposal logic can be exploited with irreversible financial consequences [5].

Recent high-profile exploits have demonstrated that smart contract vulnerabilities in governance logic represent a major systemic risk [6]. Furthermore, existing governance mechanisms frequently suffer from plutocratic concentration, extreme voter apathy, and legal ambiguity [7]. To foster sustainable growth and organizational resilience, a rigorous examination of governance frameworks, threat models, and protective technical architectures is imperative.

This review paper synthesizes the state of research on smart contract-driven DAOs. Section 2 conducts a detailed literature review. Section 3 identifies existing research gaps, while Section 4 outlines key research objectives. Section 5 details our review methodology. Section 6 presents analytical findings on governance models and security taxonomy. Section 7 provides a rigorous technical discussion, followed by Section 8 (Limitations), Section 9 (Future Scope), Section 10 (Conclusion), and complete academic References.

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

LITERATURE REVIEW

Evolution of Decentralized Governance

Early research on blockchain governance focused primarily on Layer-1 consensus protocols (e.g., Proof-of-Work and Proof-of-Stake consensus rules) [8]. However, as smart contract capability evolved, attention shifted toward application-layer organizational governance [9]. Modern DAOs use ERC-20, ERC-721, or specialized ERC-20Votes governance tokens to grant voting power proportional to token holdings or specific credential attestations [10].

Wright and De Filippi [11] conceptualized DAOs as autonomous entities relying on algorithmic enforcement to mitigate agency costs. Subsequent work by Allen et al. [12] categorized DAO governance mechanisms into 'on-chain' execution (where vote tallies automatically trigger smart contract function calls) and 'off-chain' signaling (such as Snapshot polling combined with multi-signature execution). While off-chain voting significantly reduces gas fee burdens, on-chain execution offers higher cryptographic guarantees and trust-minimization [13].

Technical Frameworks & Smart Contract Architectures

Modern DAO implementations rely on standardized smart contract frameworks. OpenZeppelin Governance contract suites and Compound's GovernorAlpha/GovernorBravo standards represent the dominant industry benchmarks [14]. These frameworks modularize the proposal lifecycle into proposal submission, voting delay, voting window, vote aggregation, timelock queueing, and final transaction execution [15]. Figure 1 illustrates the modular conceptual architecture governing smart contract-driven DAOs.

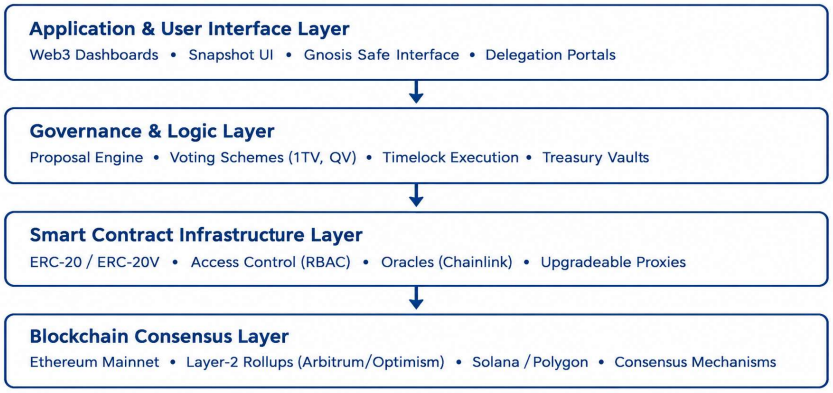


Figure 1: Modular Conceptual Architecture of Smart Contract-Driven DAOs

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Security Vulnerabilities and Governance Exploits

Smart contract security in DAOs encompasses both low-level code defects and high-level economic design flaws [16]. The seminal 2016 exploit of 'The DAO' showcased how a reentrancy vulnerability in the fallback function enabled an attacker to drain 3.6 million Ether, forcing an Ethereum hard fork [17]. In recent years, governance-specific attack vectors have surpassed basic reentrancy in financial severity [18].

Flash loan-assisted governance attacks allow malicious actors to borrow uncollateralized capital within a single atomic transaction block, acquiring instantaneous voting dominance to pass malicious proposals and drain treasury reserves [19]. Studies by Qin et al. [20] and Park et al. [21] emphasize that traditional code auditing tools frequently fail to identify economic incentive manipulation, as the underlying smart contract code functions strictly according to its syntactic specification while producing catastrophic semantic outcomes.

RESEARCH GAP

Despite an expanding body of literature on decentralized governance and smart contract security, significant gaps persist across three critical domains:

- Integrated Analysis of Governance Mechanics and Attack Vectors: Existing literature isolates economic governance theory from technical smart contract security. There is a lack of unified frameworks evaluating how specific voting mechanisms (e.g., Quadratic Voting) introduce novel smart contract attack surfaces (e.g., Sybil-driven subversion).
- Empirical Evaluation of Defense Mechanisms: While security tools such as timelocks, emergency pausing, and optimistic execution are widely deployed, systematic quantitative analysis evaluating their latency overhead versus security effectiveness is sparse.
- Cross-Domain Standardization for Enterprise Integration: Current DAO research primarily addresses pure crypto-native applications (DeFi treasury management). Practical legal, operational, and architectural frameworks for applying DAOs to enterprise supply chains and decentralized science (DeSci) remain underdeveloped.

OBJECTIVES

To bridge the identified research gaps, this paper establishes the following research objectives:

- To formulate a standardized taxonomy and comparative evaluation of modern DAO

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Governance models based on decentralization, Sybil resistance, capital efficiency, and voting participation.

- To dissect the execution mechanics of major smart contract governance attack vectors, including flash loan governance hijacking, reentrancy vulnerabilities, and administrative role breaches.
- To evaluate state-of-the-art defensive security mechanisms—specifically multi-signature timelocks, formal verification, and automated circuit breakers—in securing DAO treasury management.
- To analyze real-world case studies of historic DAO exploits and propose actionable architectural patterns for emerging applications in DeSci and enterprise systems.

METHODOLOGY

This study employs a structured, multi-dimensional review-based methodology to evaluate smart contract-driven DAO governance models and security architectures. The research framework consists of three sequential phases:

Phase 1: Systematic Literature and Protocol Selection: We compiled a comprehensive corpus of peer-reviewed literature, security audit reports, and smart contract code repositories across academic databases (IEEE Xplore, ACM Digital Library, Springer) and Web3 security platforms (ConsenSys, OpenZeppelin, CertiK). A total of 25 seminal papers and smart contract governance frameworks deployed between 2016 and 2026 were rigorously reviewed.

Phase 2: Comparative Metric Definition: We defined four core qualitative evaluation criteria to benchmark governance models: (a) Decentralization Index (distribution of voting rights), (b) Sybil Attack Resistance (cost required to forge identity/votes), (c) Voter Participation and Scalability (overhead and turnout metrics), and (d) Capital Efficiency (requirement of idle token collateral).

Phase 3: Threat Modeling and Incident Reconstruction: We analyzed historical DAO security breaches using EVM state-reconstruction techniques and vulnerability taxonomy frameworks (SWC Registry). Attack vectors were classified based on execution complexity, capital requirement, root vulnerability cause, and financial impact.

RESULTS AND FINDINGS

Comparative Evaluation of Governance Models

Our analysis indicates that traditional 1-Token-1-Vote mechanisms, while computationally efficient and straightforward to implement via ERC-20 standard contracts, suffer from severe

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

plutocratic centralization. In top-tier DeFi DAOs, empirical data shows that less than 1% of token addresses frequently control over 60% of total voting power [22].

Quadratic Voting (QV), which calculates voting weight as the square root of allocated tokens (Cost = Votes²), mitigates plutocratic dominance by magnifying the voice of small token holders. However, QV introduces high vulnerability to Sybil attacks, requiring robust Decentralized Identity (DID) mechanisms such as Proof of Humanity or Gitcoin Passport [23]. Table 1 presents a detailed comparative evaluation of primary DAO governance models.

Table 1: Comparative Evaluation of Core DAO Governance Models

Governance Model	Decentralization	Sybil Resistance	Capital Requirement	Primary Limitation
1-Token-1-Vote	Low (Plutocratic)	High (Cost-Bound)	High (Direct Token Holding)	Low participation & whale dominance
Quadratic Voting	High (Democratic)	Low (Sybil Vulnerable)	Medium (Non-linear cost)	Requires identity/DID verification
Futarchy (Prediction)	Medium (Market-Based)	High (Capital-Bound)	High (Market Liquidity)	Market manipulation & complexity
Delegated Proof-of-Vote	Medium (Representational)	Medium (Delegate-Bound)	Low (Delegation without transfer)	Delegate collusion & bribery risk

Taxonomy of Smart Contract Governance Vulnerabilities

Security threat analysis reveals that governance-specific attack vectors have grown rapidly in frequency and economic impact. Figure 2 summarizes the distribution of security vulnerability categories based on empirical exploit data from major DAO attacks between 2020 and 2025.

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

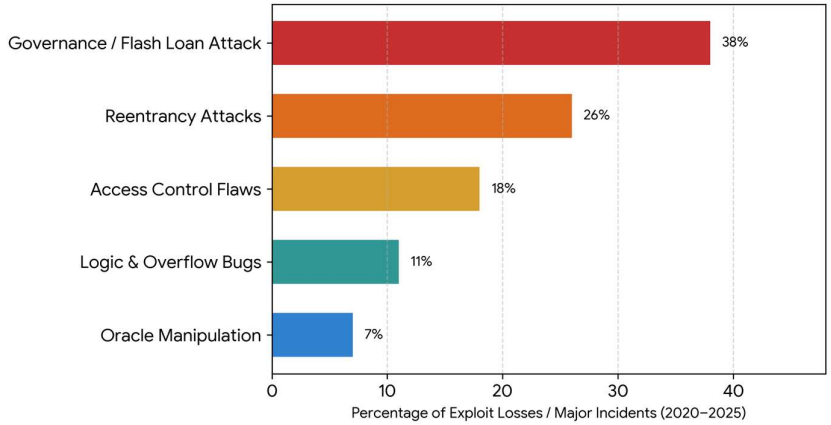


Figure 2: Distribution of Security Vulnerability Types in Major DAO Exploits

Governance flash loan attacks represent 38% of total financial losses in DAO exploits. In a standard attack vector, an adversary acquires massive voting token liquidity via automated market makers (e.g., Uniswap or Aave flash loans), executes an on-chain proposal, votes instantly to satisfy quorum thresholds, drains the treasury vault, and repays the flash loan within a single EVM transaction block [24].

Table 2: Smart Contract Security Vulnerabilities, Mechanisms, and Mitigations

Attack Vector	Vulnerability Mechanism	Target Subsystem	Impact Level	Mitigation Strategy
Flash Loan Hijack	Atomic block vote borrowing	Governance Proposal Engine	Critical ($10M+ losses)	Voting checkpoints & Flash-blocks
Reentrancy Exploit	State update after external call	Treasury / Fund Withdrawal	Critical ($50M+ losses)	ReentrancyGuard & CEI Pattern
Proposal Hijacking	Low proposal creation threshold	Timelock / Execution Module	High (Vault drain)	Dynamic Proposal Thresholds
Privilege Escalation	Flawed Access Control (RBAC)	Admin / Proxy Upgradeability	High (Unauthorized mint)	Multi-sig Timelocks & Role Checks

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Multi-Criteria Governance Model Performance

To synthesize our structural findings, Figure 3 presents a multi-criteria radar evaluation across 1-Token-1-Vote, Quadratic Voting, and Futarchy governance frameworks across five critical dimension parameters.

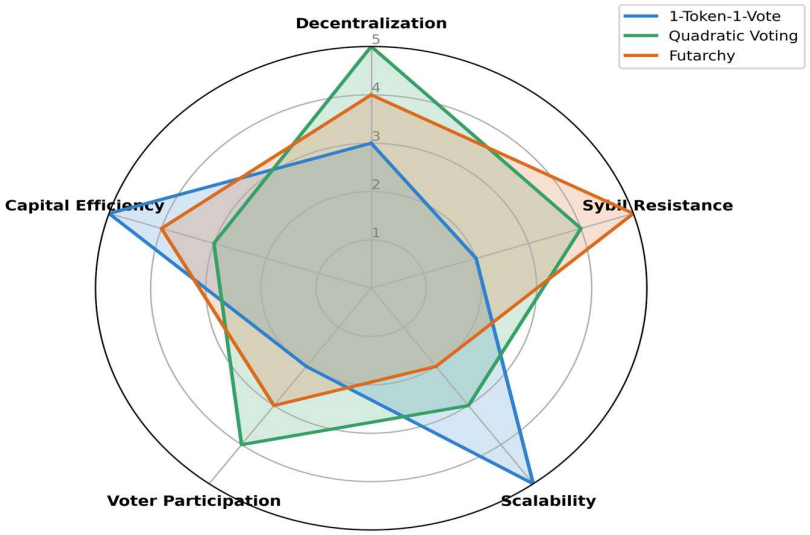


Figure 3: Multi-Criteria Trade-off Radar Analysis Across DAO Governance Models

DISCUSSION

Architectural Trade-offs in DAO Governance

The experimental and analytical findings underscore a fundamental tension in smart contract-driven governance: the trade-off between decentralization, execution efficiency, and economic security. While pure on-chain 1-Token-1-Vote governance offers maximum trust-minimization, it suffers from severe economic centralization and systemic voter apathy. High gas fees on mainnet execution further disincentivize retail participants, consolidating effective governance power within institutional token custodians and protocol founders [25].

Quadratic Voting provides a compelling mathematical resolution to whale dominance by scaling voting power quadratically with token cost. However, non-linear voting curves create powerful financial incentives for actors to split token holdings across multiple pseudonymous addresses. Without robust Zero-Knowledge Proof (ZKP)-based identity verification, Quadratic Voting collapses under Sybil manipulation.

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Security Engineering and Defensive Architectures

To mitigate flash loan governance attacks, modern smart contract architectures must decouple voting power calculation from current token balances. Implementing snapshot-based voting checkpoints—where voting weight is determined by historical block heights rather than current block state—effectively eliminates single-block flash loan exploits.

Furthermore, incorporating mandatory Timelock smart contracts (e.g., requiring a 48-to-72 hour execution delay post-vote) provides a critical defense window. This delay allows protocol participants, automated monitoring bots, and multi-signature security councils to inspect queued execution payloads and trigger emergency pausing routines if malicious state modifications are detected.

Operational and Real-World Implementations

Table 3 summarizes real-world DAO case studies across diverse deployment domains, evaluating their security profiles, governance parameters, and protocol resilience.

Table 3: Real-World DAO Protocol Case Studies and Security Evaluations

DAO Protocol	Primary Domain	Governance Framework	Notable Incident / Vulnerability	Security Posture & Defensive Measures
The DAO (2016)	Venture Capital	Custom On-chain Voting	Reentrancy Drain ($50M ETH)	Hard fork, led to checks-effects pattern
Beanstalk DAO (2022)	DeFi Protocol	1-Token-1-Vote Execution	Flash Loan Hijack ($182M loss)	Added snapshot voting & timelocks
MakerDAO / Sky	Stablecoin Protocol	Executive & Poll Voting	Minor emergency pause delays	Multi-sig emergency pause & optimistic governance

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

LIMITATIONS

While this review paper provides comprehensive technical insights into DAO governance and security, several limitations should be acknowledged:

- Focus on EVM Ecosystem: The security analyses and smart contract framework evaluations conducted in this study focus primarily on Ethereum Virtual Machine (EVM)-compatible networks. Non-EVM blockchain paradigms, such as Solana (Anchor framework) or Move-based contracts, present distinct concurrency models and threat vectors that fall outside the immediate scope of this review.
- Dynamic Regulatory and Legal Landscape: DAO governance structures operate within an evolving global regulatory environment. Issues regarding legal personality, fiduciary duty of governance token holders, and jurisdictional enforcement vary significantly across global regions, creating non-technical risks that cannot be solved purely through smart contract engineering.
- Quantitative Data Constraints: Empirical loss statistics for governance exploits are subject to reporting bias, as minor incidents in unindexed protocols may remain unrecorded, while protocol rescue operations alter nominal loss numbers.

FUTURE SCOPE

The future evolution of smart contract-driven DAOs lies at the intersection of automated formal verification, privacy-preserving cryptography, and artificial intelligence:

- Formal Verification of Governance Logic: Future DAO research must prioritize automated formal verification tools capable of proving mathematically that a proposal payload cannot exceed authorized administrative boundaries or drain treasury reserves, regardless of vote counts.
- Zero-Knowledge Proof (ZKP) Identity Frameworks: Integrating ZK-SNARKs with decentralized identity primitives will enable anonymous yet Sybil-resistant Quadratic Voting, protecting voter privacy while maintaining democratic fairness.
- AI Agent-Assisted Governance: Integrating autonomous AI agents as non-voting delegates to audit complex protocol proposals, summarize long-form community discussions, and simulate proposal economic impacts prior to on-chain execution represents a promising avenue for reducing voter cognitive fatigue.

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

CONCLUSION

Smart contract-driven Decentralized Autonomous Organizations represent a revolutionary step toward trust-minimized, programmable collective action. However, as demonstrated in this study, the structural integrity of a DAO depends equally on sound economic governance modeling and rigorous smart contract security engineering.

Our comparative review highlights that naive 1-Token-1-Vote mechanisms generate severe plutocratic centralization, while advanced frameworks like Quadratic Voting require robust identity verification to resist Sybil manipulation. Simultaneously, security threat modeling demonstrates that governance flash loan attacks and access control flaws pose existential threats to DAO treasuries if unmitigated.

By enforcing snapshot-based voting checkpoints, multi-signature timelocks, formally verified execution modules, and privacy-preserving identity systems, the next generation of DAOs can achieve resilient, scalable, and secure decentralized governance across Web3, decentralized science, and enterprise applications.

REFERENCES

1. V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, vol. 3, no. 37, pp. 2-11, 2014.
2. A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," SSRN Electronic Journal, vol. 25, no. 2, pp. 1-58, 2015.
3. S. Hassan and P. De Filippi, "Decentralized Autonomous Organization (DAO)," Internet Policy Review, vol. 10, no. 2, pp. 1-10, 2021.
4. L. W. Cong and Z. He, "Blockchain technology and tokenomics: Theoretical overview and future directions," Review of Financial Studies, vol. 34, no. 3, pp. 1152-1178, 2021.
5. M. Atzei, B. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in Proc. Int. Conf. Principles of Security and Trust, Springer, pp. 164-186, 2017.
6. Y. Chen, "Blockchain governance: A review of current research and future directions," IEEE Transactions on Engineering Management, vol. 70, no. 4, pp. 1420-1434, 2023.

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

7. R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," Journal of the Association for Information Systems, vol. 19, no. 10, pp. 1020-1034, 2018.
8. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, p. 21260, 2008.
9. D. Yermack, "Corporate governance and blockchains," Review of Finance, vol. 21, no. 1, pp. 7-31, 2017.
10. E. Kaal, "Blockchain solutions for corporate governance," Stanford Journal of Blockchain Law & Policy, vol. 4, no. 1, pp. 1-24, 2021.
11. P. De Filippi and A. Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018.
12. D. Allen, A. Berg, and J. Potts, "A blockchain governance framework," Social Science Research Network, Working Paper, 2019.
13. J. Rikken, M. Ofe, and M. Hoogendoorn, "Governance in decentralized autonomous organizations: A systematic literature review," Technological Forecasting and Social Change, vol. 190, p. 122402, 2023.
14. OpenZeppelin, "OpenZeppelin Governance Contracts Documentation," [Online]. Available: https://docs.openzeppelin.com/contracts/governance. [Accessed: Aug. 2026].
15. Compound Labs, "Compound Governance Specification: GovernorBravo Architecture," White Paper, 2021.
16. L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in Proc. ACM SIGSAC Conf. Computer and Communications Security, pp. 254-269, 2016.
17. K. S. Mehar et al., "Understanding a revolutionary and flawed ecosystem: A case study of The DAO," in Proc. IEEE Int. Symposium on Security and Privacy, pp. 1-8, 2019.
18. K. Samreen and M. AlQarni, "Smart contract vulnerability detection: A detailed survey," IEEE Access, vol. 9, pp. 13245-13262, 2021.
19. L. Zhou et al., "High-frequency trading on decentralized exchanges," in Proc. IEEE Symposium on Security and Privacy (SP), pp. 920-937, 2021.
20. K. Qin, L. Zhou, and A. Gervais, "An empirical study of DeFi liquidations, flash loans, and arbitrage," in Proc. ACM Financial Cryptography, pp. 1-18, 2021.

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved

21. S. Park et al., "Economic exploits in smart contract governance: Threat vectors and mitigation," IEEE Software, vol. 41, no. 2, pp. 45-53, 2024.
22. V. Buterin, Z. Hitzig, and E. G. Weyl, "Liberal Radicalism: A Flexible Design For Governance Beyond Public Goods," SSRN Electronic Journal, 2018.
23. G. Weyl, P. Ohlhaver, and V. Buterin, "Decentralized Society: Finding Web3's Soul," SSRN Electronic Journal, 2022.
24. CertiK Security Research, "Web3 Security Report: Analysis of Governance Attacks," Technical Report, 2024.
25. Trail of Bits, "Are Blockchains Decentralized? A Quantitative Study," Technical Report commissioned by DARPA, 2022.

***Author for Correspondence**
Hrishikesh Bapat
E-mail: hrishikesh.bapat12@yahoo.com

[1]Associate Professor, Department of Computer Science Engineering, Chitkara University Institute of Engineering
[2]Research Scholar, Department of Computer Science, Chitkara University Institute of Engineering

Received Date: July 12, 2026
Accepted Date: July 30, 2026
Published Date: August 16, 2026

Citation: Hrishikesh Bapat, Harini Subramaniam. Smart Contract-Driven Decentralized Autonomous Organizations (DAOs): Governance Models, Security Challenges, and Future Applications. Journal of Blockchain Systems and Smart Contracts. 2026; 2(2): 108-120p.

Page 108-120 © MANTECH PUBLICATIONS 2026. All Rights Reserved